UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

STEVEN FLOYD, Plaintiff(s), v. AMAZON.COM INC., et al., Defendant(s).	CASE NO. C22-1599-KKE ORDER ON JOINT STATEMENT OF DISPUTES REGARDING A PROTECTIVE ORDER

This matter comes before the Court on the parties' joint statements of disputes regarding a protective order. Dkt. Nos. 53, 76.[1] The Court heard the oral argument on these issues on November 8, 2023 (Dkt. No. 70), and the Court again commends the parties for working together to narrow the disputes remaining for resolution. For the reasons explained herein, the Court finds that Defendants' proposed protective order appropriately safeguards protected material without imposing undue practical burdens.

I. BACKGROUND

Plaintiff filed a class-action complaint asserting a violation of the Sherman Act in November 2022 and amended his complaint in February 2023. Dkt. Nos. 1, 37. Defendants' motion to dismiss was granted in part and denied in part in June 2023 (Dkt. No. 61), and discovery commenced the following month. *See* Dkt. No. 67 at 1.

[1] This order refers to the CM/ECF page numbers of the parties' submissions.

The parties assert that entry of a protective order will greatly assist them in proceeding with discovery. Dkt. No. 67 at 5. They have agreed upon many aspects of a protective order, but certain disputes remain. Specifically, the parties could not reach agreement as to provisions on data security and access to protected materials outside the United States and by foreign nationals. *See* Dkt. No. 76.

II. LEGAL STANDARDS

Under Federal Rule of Civil Procedure 26(c), a court may enter a protective order upon a showing of good cause that protection is needed. Courts have discretion to fashion an order to protect a party, or person, from annoyance, embarrassment, oppression, undue burden, or expense. *See* Rule 26(c)(1). "A trial court possesses broad discretion in issuing a protective order and in determining what degree of protection is required." *Sec. & Exch. Comm'n v. R.J. Reynolds Tobacco Holdings, Inc.*, No. MISC.A.03-1651(JDB), 2004 WL 3168281, at *9 (D.D.C. June 29, 2004).

III. DATA SECURITY

The parties' first dispute centers on the extent of data security measures needed to adequately protect the "voluminous amount of confidential information requested and ultimately produced in this nationwide class action litigation." Dkt. No. 76 at 7. Defendants propose multiple additional layers of protection beyond what is contemplated in this district's model protective order, and while Plaintiff is now willing to stipulate to most of these additions, Plaintiff objects to three of Defendants' proposed measures, which the Court will address in turn.

A. Information Security Management System

First, Plaintiff objects to Defendants' proposal that the parties (and anyone else accessing protected material) implement data management systems complying with established data security frameworks. *See* Dkt. No. 76-2 § 9(1) (requiring the parties to "implement an information security

management system ('ISMS')" that complies with one of three standards or, as a fourth catchall option, "the most recently published version of another widely recognized industry or government cybersecurity framework"). Plaintiff contends that the three example frameworks listed in Defendants' proposal are complex, confusing, and highly detailed, but does not explain why the fourth catchall option could not be utilized to implement a less onerous but nonetheless secure system. Dkt. No. 76 at 3–4.

To the extent that Plaintiff also argues that it would be burdensome to require individuals or experts to comply with the ISMS requirement (Dkt. No. 76 at 4), Plaintiff has not explained why an exception is warranted here. Defendants' proposal safeguards protected material via industry-standard requirements, and Plaintiff has offered no justification for creating a loophole for third parties.

B. Data Breach

Second, Plaintiff objects to Defendants' proposal regarding actions to be taken in response to a data breach. Defendants propose that the parties must "submit to reasonable discovery" in the event of a data breach, and list other potential actions that may be taken as well. *See* Dkt. No. 76-2 at § 9(4) (stating that the parties must meet and confer to determine any adjustments to be made in light of the data breach, "potentially including but not limited to" specific actions). Plaintiff contends that listing "'potential' actions serves no purpose other than to prejudge the appropriate response." Dkt. No. 76 at 5. Plaintiff has not shown that any of the potential actions listed are inappropriate, however. Because Defendants' proposal requires the parties to meet and confer about whether actions are appropriate, Plaintiff will have an opportunity to negotiate the appropriate course of action as needed and the Court finds no reason to exclude a non-exhaustive list from this section. To the extent that Plaintiff contends that "[f]ormal discovery may not be appropriate" (Dkt. No. 76 at 5) after a data breach, again, Plaintiff will have an opportunity to

discuss that matter with Defendants in determining a reasonable course of action if and when the need arises. Defendants' proposal allows the parties to craft an appropriate response based on the particular circumstances of a data breach, and Plaintiff has not shown that the proposal is burdensome or unworkable.

C. Multi-Factor Authentication

Third, Plaintiff objects to Defendants' proposal that the parties must implement multi-factor authentication for *any* access to protected materials. *See* Dkt. No. 76-2 § 9.1 ("The Parties shall implement multi-factor authentication for any access to Protected Materials." (footnote excluded)). Plaintiff contends that this requirement is "ambiguous and, read literally, could require contemporaneous multi-factor prompts every time Protected Material is reviewed." Dkt. No. 76 at 5. Instead, Plaintiff proposes a less stringent multi-factor authentication requirement that does not explicitly apply to each attempt to access protected materials. *See* Dkt. No. 76-1 § 9.1 ("The Parties shall implement multi-factor authentication tools to prevent unauthorized access to Protected Materials." (footnote excluded)). The Court finds that Defendants' proposal promotes consistency, and that Plaintiff has not shown that this commonplace security measure is unnecessary whenever protected material is accessed.

IV. ACCESS OUTSIDE THE UNITED STATES AND BY FOREIGN NATIONALS

Defendants propose that protected material be stored and maintained in the United States only, and that remote access to the material from outside the United States should be limited to view-only access from the server located within the United States. *See* Dkt. No. 76-2 § 5. Defendants also seek to prohibit physically or electronically transporting protected materials to experts or consultants who are either located outside the United States or are foreign nationals. *See id*. §§ 5.2(b), 5.6. Defendants contend this prohibition is necessary to avoid running afoul of

export regulations as well as the "risk of transporting confidential materials outside the country where the actors are not subject to this Court's jurisdiction." *See* Dkt. No. 76 at 11.

To address these concerns, Plaintiff propose that Defendants identify at the time of production particular documents that should not be physically or electronically transmitted outside the United States, and at that point Plaintiff may object and potentially seek Court intervention if agreement cannot be reached. *See* Dkt. No. 76-1 § 5.6. Plaintiff has not explained why this process is necessary, if foreign experts or consultants can view the protected material remotely. Although Plaintiff raises productivity concerns (Dkt. No. 76 at 7), at this time the Court finds no basis to conclude that this concern outweighs the safeguard achieved by Defendants' proposal. Without a persuasive showing that remote access is insufficient, the Court declines to require the parties to engage in continued negotiation on this issue. In the event this provision results in actual, significant, and demonstrated burdens on the productivity of Plaintiff's experts or consultants, Plaintiff may petition the Court to revisit this issue on a fuller record.

V. CONCLUSION

For these reasons, the Court resolves the parties' remaining disputes in Defendants' favor. Defendants are ORDERED to submit their proposed protective order to the Court at EvansonOrders@wawd.uscourts.gov for entry, and the clerk is directed to TERMINATE the parties' statement of disputes (Dkt. No. 53).

Dated this 15th day of December, 2023.

Kymberly K. Evanson
United States District Judge